HOW TO EFFECTIVELY MEASURE & COMMUNICATE THE PROGRESS OF YOUR VULNERABILITY MANAGEMENT PROGRAM

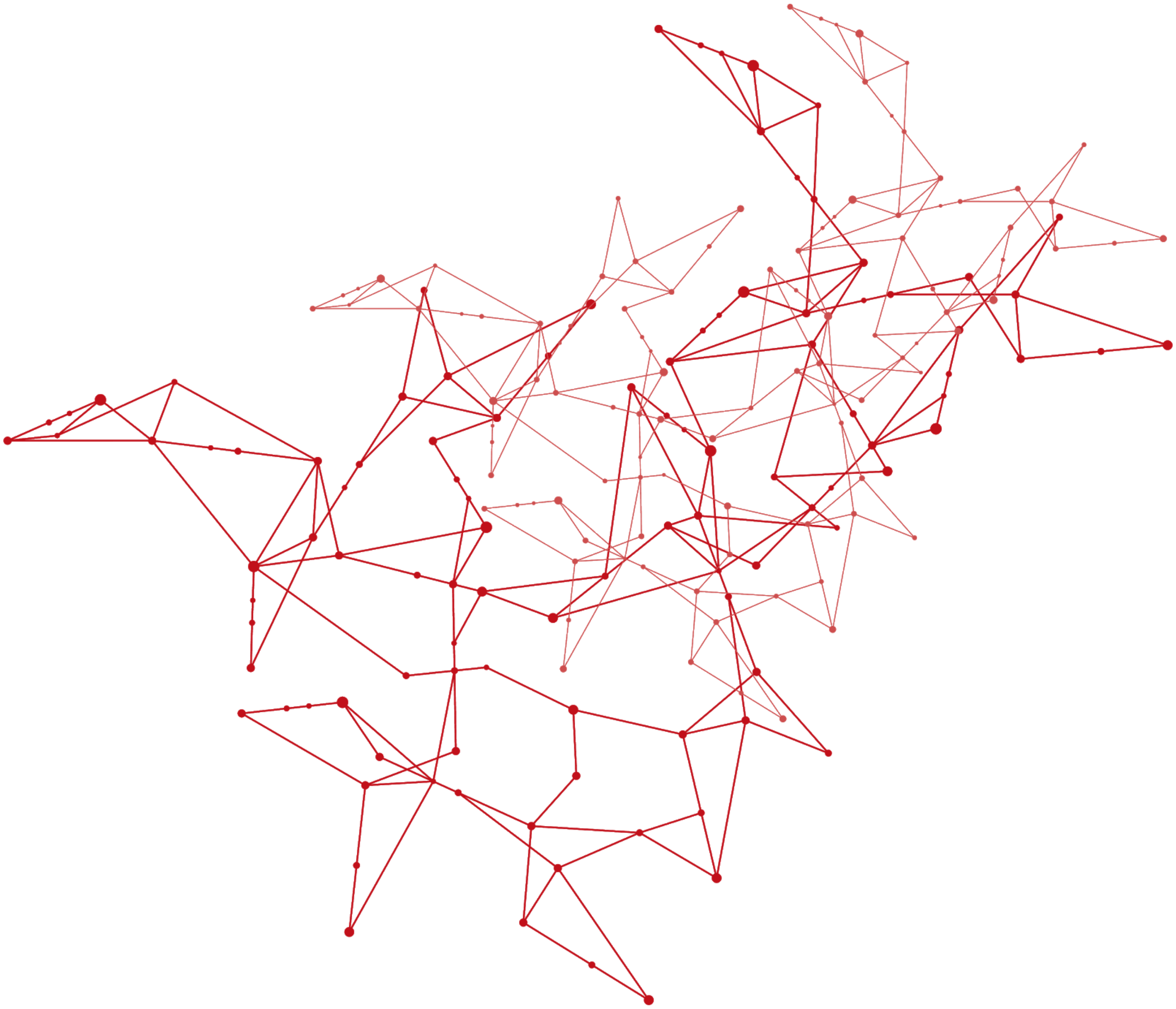
A Comprehensive Guide for VM Program Owners

TABLE OF CONTENTS

SUMMARY

In this white paper, vulnerability management program owners will learn how to:

- Track the progress of the VM program, while saving both time and money
- Partner-up and align with the IT team on goals to push the program forward
- Communicate results of the VM program to executives and board members



CHALLENGES OF MEASURING & REPORTING ON VM PROGRESS

Vulnerability management (VM) is as much about people and processes as it is about technology. Not only does it incorporate the full scope of remediation, but it also requires managing workflow and communication across teams. A successful vulnerability risk management program is one that:

- Proactively **informs** the organization about risks and progress
- **Prioritizes** and focuses on fixing the most critical vulnerabilities
- Ensures **continuous** operational efficiency, while saving time wherever possible

Today, vulnerability management is gaining traction as a necessary preventative measure to reduce risk. However, measuring, executing, and reporting on the program remains a challenge.

Why?

1. Miscommunication With Executives

Communicating the health of the VM program outside of security and IT teams is often difficult. Most people aren't well-versed in the language of information security—especially those heavily focused on business. For the program to be effective, VM leaders must be able to clearly demonstrate progress in a way that the executive team and board members understand.

2. Misalignment Between IT & Security

Vulnerability management also requires a strong partnership between security and IT to achieve the ultimate goal of reducing risk and protecting the most business-critical assets. As the primary drivers of remediation, these groups must align on goals and processes—though they don't always see eye to eye.

3. Manual & Infrequent Measurement

Many enterprises still execute VM manually, using Excel spreadsheets and sending individual emails to asset owners. This only convolutes the workflow and adds more time to the remediation process. Not to mention, enterprise networks are in a constant state of change, meaning frequent scans are more important than ever.

THE CURRENT VULNERABILITY MANAGEMENT LANDSCAPE

Before tackling the problems with measuring and reporting on the health of the vulnerability management program, it's important to understand the root cause. The challenges mainly stem from a combination of:

- **Constant environmental changes** in the enterprise technology landscape
- The **early maturity level** (and manual execution) of many enterprise VM programs

Keeping Up With Modern Dynamic Environments

With digital transformation, an explosion of mobile and connected devices, and the constant release of new cloud and software services, the VM landscape grows more complex every day. In fact, the available enterprise attack surface is growing faster than it has at any other point in history[1]. Meanwhile, dozens of new vulnerabilities each day. Without the most recent and relevant asset data, VM teams won't know how to protect the business. That said, it's no longer enough to measure how healthy the organization is *today*. It's also important to know how risks increase or decrease *over time*.

[1] https://cdn2.hubspot.net/hubfs/486579/Avast_Threat_Landscape_Report_2019.pdf

Historically, vulnerability management has been conducted on a project basis. But because enterprise networks are in a constant state of change, the program must run continuously. This requires full coverage of known and unknown assets at the same rapid pace of environmental changes. Unfortunately, many enterprises haven't reached a level of VM maturity to measure what they need to improve[2].

Dozens of new vulnerabilities are discovered each day.

Traditional VM Methods Are Inefficient

Numerous enterprises still conduct vulnerability management manually. For instance, many use Excel spreadsheets to track, analyze, deduplicate, and prioritize vulnerabilities. Some even assign vulnerabilities via email, which often requires additional follow up.

These manual methods are neither practical nor scalable due to the large number of assets and network changes in enterprises. With no shortage of vulnerabilities, there's already too much work on top of limited time and resources. Organizations simply can't afford to lose any more time in the process when critical assets are at stake.

Likewise, these manual processes are costly. Information Security employees (analysts in particular) are expensive to hire. Their jobs are also in high demand, meaning they won't think twice about leaving if they're unhappy at work. Working manually in spreadsheets all day long is surely enough to make them look for other opportunities. Organizations can't afford this kind of turnover, especially in the midst of a cybersecurity talent shortage[3].

[2] https://www.nopsec.com/time-is-money-part-1/

[3] https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

PROGRESS: THE METRIC THAT MATTERS MOST

With a clearer understanding of what's causing today's challenges with vulnerability management, it's time to dive into the solution. Let's start with *what* to measure.

In addition to technology, vulnerability management heavily focuses on managing people and processes. With valuable data on the line, the entire organization should understand the security risks involved and their role in it—whether it's the security team, IT team, or senior executives and board members. Likewise, all stakeholders should be looking at both the problem and processes the same way. And there should be a single source of truth for how the program is performing. We'll refer to this as simply, **progress**.

From a VM perspective, progress can be further defined as remediating the most critical vulnerabilities, reducing attack surface, mitigating environmental damage, and minimizing overall business risk. Progress is demonstrated when the *right* vulnerabilities (that pose the greatest threat) are fixed *and* when risk reduces over time.

Why is progress the best metric to focus on? For one, progress indicators help expose both working and broken processes so the VM team can continually improve the program.

Progress as a metric is also broad and simplified enough to report in any context, across departments. Developing a repeatable process for reporting on the organization's risk posture helps ensure everyone understands their role in remediation—whether that means the IT team patching or the C-suite deciding budget and headcount.

So, how can you ensure progress is understood the same way across all teams? First, everyone needs to align on the goals of the program, starting with security and IT—two groups who have a history of friction and misalignment.

IT & SECURITY:

A NECESSARY PARTNERSHIP

IT and security are both key to minimizing organizational risk. In the event of a data breach or security threat, these teams must work together to remediate as soon as possible, particularly as enterprise networks grow more complex.

Unfortunately, each group has different objectives. While security is most concerned potential risks and vulnerabilities, IT cares more about availability, speed, and stability. And while security sees the worst possible outcome as a *breach*, IT views it as *downtime*. Because security measures often slow things down, the vulnerability management program is often seen as a productivity roadblock for IT. For instance, there's often pushback during remediation because patching is often seen as risky or disruptive by developers and IT administrators.

These conflicting goals make getting IT on board with vulnerability management a struggle.Yet as security already lacks jurisdiction into what IT works on, this buy in is necessary.

For the program to succeed, these two groups must align on goals and processes. Both should focus on the overall mission: to protect the confidentiality, integrity, and availability of the company's most critical assets.

Collaboration and alignment between security and IT is critical.

The best solution to this problem is better communication. Each team should proactively discuss issues and update each other on a daily basis—not just when disaster strikes.

HOW TO MEASURE & REPORT ON VM PROGRESS

Once it's clear what to track and security and IT align, it's time to start measuring and communicating progress to executives.

It's important to note that raw vulnerability data in itself isn't useful insight for improving the program—especially when reporting to executives. Upper management doesn't need to know *everything*, nor will they understand what all of the data actually means. While security and IT teams may need to know about the technicalities of a vulnerability, the C-suite just needs to know the risks posed to the business.

The key to quantifying and relaying vulnerability management progress is therefore focusing on the right metrics for the audience. With this in mind, let's discuss the appropriate steps for measuring and reporting on the health of the program:

1. Set SMART Goals

A successful vulnerability management program starts with clear goals related to business objectives, agreed upon by all stakeholders. First, determine which assets are most important to the organization and set specific, measurable, attainable, relevant, and timely (SMART) goals for protecting these assets[4]. From there, you can start establishing baseline metrics to measure improvement.

2. Focus on the Right Metrics

Data means different things to different people. When demonstrating progress, VM leaders should be able to turn vulnerability data into meaningful insights that can be understood across teams. The metrics measured and reported should be simple, repeatable, and create shared learnings across the organization.

[4] https://blog.isc2.org/isc2_blog/2013/02/define-smart-it-security-goals.html

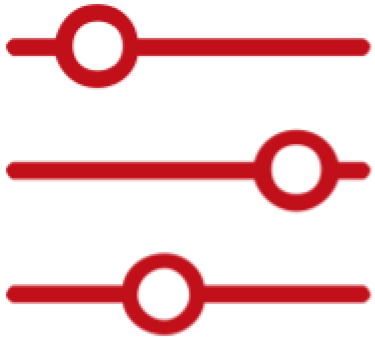
A common point of mistranslation occurs between executive teams and technical teams like InfoSec and IT. C-level and board stakeholders ultimately want to understand the organization’s risk posture, or the likelihood a threat will be exploited and the potential impact of the vulnerability on the business. They likely don’t have the knowledge to interpret comprehensive technical data, and providing too much detail will only muddle the message.

The reporting should be strictly focused on the impacts to the business—a language executives know well. Being said, VM leaders should be able to clearly relay at a *high level* the following to executive stakeholders:

- where the organization stands in terms of security
- how current risk levels compare with previous months
- what progress is being made to reduce risk

3. Emphasize the Focus on Impact, Not Count

Any security or vulnerability manager knows that there’s no shortage of vulnerabilities. They also know that there’s not enough time or resources to find and fix *every* vulnerability. Yet this is often what board of directors and C-suite members expect.



Focus on *impact*, not count when measuring and reporting.

Vulnerability management has been historically treated as a numbers game, tracking progress by counting the number of closed vulnerabilities. But this is impractical given that large enterprises could have tens of thousands of assets and tens of millions of vulnerabilities, with more discovered each day. Besides, the quantity will only increase as more assets accumulate. Even if the VM team only focused on the 2% of vulnerabilities that actually get exploited[5], it’s too much to handle in such a time-sensitive process.

[5] https://www.nopsec.com/nopsecs-2018-state-of-vulnerability-risk-management-report/

Vulnerability managers should be able to set expectations about the remediation process to upper management. It’s essential to be transparent that not *every* vulnerability will be fixed because that would be an inefficient use of time and resources. Not to mention, not all vulnerabilities are created equal. Some pose a severe threat while others only pose a theoretical risk. Ultimately, counting closed vulnerabilities doesn’t consider the criticality of the vulnerabilities or the assets themselves.

Rather, it should be emphasized that the VM team is focusing on the most *critical* vulnerabilities that affect the most *crucial* assets, and will have the greatest *impact* on the business if exposed. It should be clear why security and IT teams must instead prioritize remediation efforts by targeting the riskiest vulnerabilities first and only move down as resources permit.

Not only is this an easier approach to managing vulnerabilities, it also ensures executives that the VM program is making efforts towards securing the business. The last thing the C-suite wants is to make the news headlines for a security breach. Highlighting that the *right* risk is getting reduced will give them confidence that the team is minimizing the negative impact on the business—even if they aren’t able to address *every* vulnerability.

MOVING TOWARDS CONTINUOUS IMPROVEMENT

With a better understanding of how to measure and communicate the health of the vulnerability management program, it’s time to focus on the future. The executive team doesn’t just care about current progress—they also want to know that progress is developing over time. They care about the bigger picture: how processes are improving and how effectively security and IT teams are working together to improve remediation for years to come. Simply put, they want to know that their business has a sustainable future. In vulnerability management, one of the clearest indicators that processes are improving is **time**.

Time is Money, Time Saved is Progress

Protecting the organization against vulnerabilities is both a time-*sensitive* and time-*consuming* process.

For one, to secure the future of the business and assets, the most critical vulnerabilities need to be removed from the system as soon as possible. Otherwise, the organization's data could be compromised and the business could fall apart. Plus, continuously managing and remediating vulnerabilities is difficult in itself and therefore takes up a lot of time.

VM is time-*sensitive* and time-*consuming*.

Conducting vulnerability management manually and/or on separate platforms complicates the workflow even further by adding additional steps and procedures. When you're already tight on resources, you not only can't afford to lose time, but you must ensure actions are taken to save time wherever possible.

To better visualize how saving time translates to progress, consider these benefits:

Reduced Risk

By running the VM program **continuously** and addressing similar vulnerabilities over time, engineers get better and faster at fixing them. The C-suite sees that progress is being made in terms of time to remediation and the organization stays ahead of attacks.

Increased Productivity

By **automating** tasks like analysis, assignments, deduplication, and prioritization, engineers can shift their focus from reactive patching and bug fixing to higher-value tasks. This means they have more time to focus on more productive things like developing new features or solutions that generate new revenue.

Continuous Improvement

Managing the entire VM program in a **single platform** allows for shared learnings that lead to more rapid execution. For example, when two engineers working on separate assets are tasked with remediating the same vulnerability, they can help each other fix it faster. Let's say Apache Struts is listed as a vulnerability on two separate assets. The engineer more experienced with Java and quicker at remediating the vulnerability can provide guidance to the less-experienced engineer. The experience can be shared, therefore speeding the process.

Cost Savings

Not only is time valuable for the security of the organization, but to upper management time is quite literally money. Time savings translate to monetary cost savings when you consider the worth of an employee's time[6]. By demonstrating improvement in terms of time spent on remediation and workflow, you're also demonstrating monetary return on investment.

CONCLUSION

Measuring and reporting on vulnerability management progress is no easy feat. The evolving enterprise technology landscape and reliance on manual processes only magnify the challenges.

Since it's key that the entire organization has a clear understanding of risk posture, strategic alignment and effective communication are paramount. First, there needs to be a strong partnership between IT and security, which requires aligning behind a common goal and definition of success. Moreover, for the executive team to understand security information, it needs to be presented in business terms with clear emphasis that the *right* risk is getting reduced.

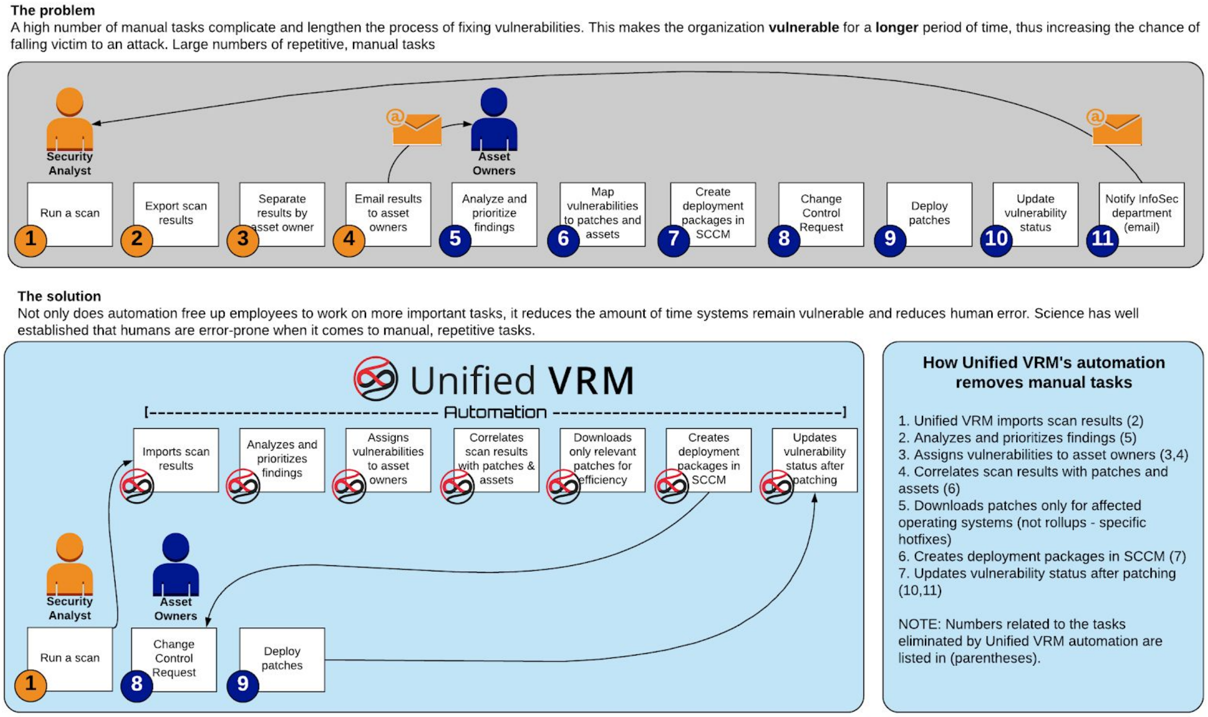
Finally, to ensure the business has a sustainable future, there needs to be a focus on continuous improvement. Because vulnerability management is both time-sensitive and

[6] https://www.nopsec.com/time-is-money-part-6/

time-consuming, this starts with refining processes and saving time wherever possible. Doing so will ultimately reduce risk, minimize cost, and increase productivity.

NopSec's Unified VRM helps enterprises achieve this with:

- **Automation:** Cutting out manual tasks such as analysis, deduplication, prioritization, assignments, and ticketing saves both time and money.
- **Visibility:** By ingesting, correlating, and deduplicating vulnerabilities into a single prioritized view, VM teams get better insight into the health of the program.
- **Prioritization:** By narrowing down the list of vulnerabilities and assigning risk scores, VM teams know what's most important to fix.



The problem

A high number of manual tasks complicate and lengthen the process of fixing vulnerabilities. This makes the organization **vulnerable** for a **longer** period of time, thus increasing the chance of falling victim to an attack. Large numbers of repetitive, manual tasks

Security Analyst
Asset Owners
1 Run a scan
2 Export scan results
3 Separate results by asset owner
4 Email results to asset owners
5 Analyze and prioritize findings
6 Map vulnerabilities to patches and assets
7 Create deployment packages in SCCM
8 Change Control Request
9 Deploy patches
10 Update vulnerability status
11 Notify InfoSec department (email)

The solution

Not only does automation free up employees to work on more important tasks, it reduces the amount of time systems remain vulnerable and reduces human error. Science has well established that humans are error-prone when it comes to manual, repetitive tasks.

Unified VRM
[---------------------------------- Automation ----------------------------------]
Imports scan results
Analyzes and prioritizes findings
Assigns vulnerabilities to asset owners
Correlates scan results with patches & assets
Downloads only relevant patches for efficiency
Creates deployment packages in SCCM
Updates vulnerability status after patching
Security Analyst
Asset Owners
1 Run a scan
8 Change Control Request
9 Deploy patches

How Unified VRM's automation removes manual tasks

1. Unified VRM imports scan results (2)
2. Analyzes and prioritizes findings (5)
3. Assigns vulnerabilities to asset owners (3,4)
4. Correlates scan results with patches and assets (6)
5. Downloads patches only for affected operating systems (not rollups - specific hotfixes)
6. Creates deployment packages in SCCM (7)
7. Updates vulnerability status after patching (10,11)

NOTE: Numbers related to the tasks eliminated by Unified VRM automation are listed in (parentheses).

Contact Nopsec today to learn how we can help you better assess and reduce vulnerability risk.

ABOUT UNIFIED VRM

NopSec's Unified VRM (Vulnerability Risk Management) is an innovative threat and vulnerability management solution that addresses the need for better prioritization and remediation of security vulnerabilities in a single platform. Powered by E3 Engine, this cloud-based SaaS platform provides visibility, prioritization, and automation throughout the whole VRM process.

Unified VRM offers an extensive array of task, workflow automation, and governance capabilities to improve remediation, drive security/IT team collaboration, and improve goal setting and management. The solution also makes reporting on current risk posture and incident status easy with rich visualizations and dashboards.

For enterprises and SMEs alike, Unified VRM helps security professionals simplify their work, effectively manage and prioritize vulnerabilities, and make informed decisions. Powered by automation and machine learning, the solution dramatically reduces the turnaround time between identification of critical vulnerabilities and remediation, helping organizations avoid attacks and costly data breaches.

> *"NopSec has an excellent understanding of the market and differentiates by offering its VRM capabilities, with or without its native scanning functionality, at compelling price points to provide value to any VRM implementation. Clients have granular control over defining system criticality, which in turn informs risk exposure scores that the platform presents well."*
>
> – The Forrester Wave™: Vulnerability Risk Management, Q1 2018

ABOUT NOPSEC

NopSec operates with one mission: to help people make better decisions to reduce security risks. Our team is passionate about building technology to help customers simplify their work, manage security vulnerability risks effectively, and empower them to make more informed decisions. Our software-as-a-service approach to vulnerability risk management offers an intelligent solution to dramatically reduce the turnaround time between identification of critical vulnerabilities and remediation.

For additional information or to schedule a demo, visit nopsec.com or email sales@nopsec.com.